OPEN DISCUSSION

Cal Pacific's Computer Camper Reports In

Thank you and California Pacific for sending me to Computer Camp. I had a great time and learned a lot. I entered a contest on the TI99/4, which I had never used before, and won first prize, which was a nylon jacket. I would have liked it to be an Apple jacket but I was happy to win it anyway.

I really enjoyed the camp and took all the classes I could. I took accelerated Basic, graphics, robotics, artificial intelligence, and game simulation. I met some real nice kids and had lots of fun. It was something I never dreamed I would get

to do. I couldn't believe I was really going to the camp until I actually got there.

I applied to the director to work as a PA next year, so I hope I make it. If I don't, I am really happy to have been able to go once anyway. My family could never have afforded to send me and it would have taken me years to save up to go if I could.

The only thing I didn't like was that they didn't have enough Apples. Some of the kids in my cabin brought their own, so that helped. Maybe you can influence them to get a few more next time and also talk Apple into making them more available.

Anyway, thanks again. I really was happy to go.

John Brandstetter, South San Gabriel, CA

Believing in Security Can Be Perilous

Being an amateur cryptographer and a member of the American Cryptogram Association, I'd like to comment on Mr. McCreary's challenge cipher. First let me state that I have no desire to win his computer system, but I am concerned about his claims.

Since I am not a regular reader of your magazine (I own a Commodore PET), this cipher was brought to my attention by a stranger who read my letter to the editor in the July 1981 issue of *Creative Computing*. There I stated that it was dangerous for anyone not familiar with advanced cryptanalytic techniques to propose an enciphering scheme which they consider "absolutely secure."

In both the preamble to the cipher and in his press releases he makes exaggerated claims of security, which are not proved even if the challenge problem is not solved. This is dangerous since sensitive data might be enciphered, creating a false sense of security, while in reality it may be very vulnerable.

As is generally known among cryptographers, security cannot rest in the secrecy of the *general* system, but in the inability to recover the *specific* keys. I therefore *challenge* Mr. McCreary to publish his complete enciphering algorithm, less specific keys, if he has such faith in the invulnerability of his scheme. Lest anyone believe this to be unfair, remember that a determined cryptanalyst with access to an Apple can get a copy of the program, and even if a listing can't be gotten, then by proper inputting to the program, the actual details of the algorithm can be slowly determined in a short time. An analogy is an inventor of a new "pick-proof" lock who won't disclose its internal workings. Again, only a careful analysis can verify such claims.

The statement in his flyer, that it is "theoretically impossible to decode without the exact duplicate key" implies that perhaps a "one-time-pad" system is used. This involves using an infinite list of perfectly random numbers as the keying sequence, which is used only once. The production of the keying sequence is important, since *truly* random numbers are hard to compile and random number generators are easily deciphered from a relatively short segment.

In addition, the key sequence must be longer than all intended messages and must be produced, transmitted, and stored under high security conditions; loss of the key compromises all information, since it can't be retrieved. In cases such as these, one might as well store the raw information and avoid the costly encipherment. Such a system was abandoned long ago by the military as being impractical under normal working conditions and has also been ruled out by all computer-cryptographers for similar reasons.

Lest anyone assume that I'm out to "get" Mr. McCreary, let me say that I'm not. If his scheme is as good as he claims then he should certainly get all the rewards; if it is not as good, then such software should see very limited use, since a false sense of security is more dangerous than no security at all. Only by an unbiased evaluation of the enciphering algorithm can such a judgment be accurately made.

Rudolph F. Lauer, Nutley, NJ

Tops despite Omission

I read with great interest Craig Stinson's survey of the various home finance packages available for the Apple computer. I am very well acquainted with most of the products he mentioned in both his articles in April and May. Although, I must confess that I was very much disappointed when his review did not cover the Apple *Personal Finance Manager*.

As I stated, I have personally tried at least 50 percent of the products surveyed, but none has shown the ease of operation I have found with the *Personal Finance Manager*.

Like most of the products surveyed,

GOTO 15

Software Sale Sets Big Bucks Record

A new level of maturation of the microcomputer software industry into big business was achieved in mid November when Personal Software acquired for cash the rights to the source code of *VisiPlot* and *VisiTrend*, the best-selling business graphing packages from Micro Finance Systems.

No actual figures on the sale were released, but the transaction was known to be in the seven-figure range, making it the largest cash transaction in microcomputer history and the largest buy of any kind of rights to source code. *VisiPlot* and *VisiTrend* had previously been marketed by Personal Software under exclusive marketing agreements.

Other large sales of microcomputer software have either involved only finished product or have involved the entire publishing company. When Peachtree bought *Magic Wand*, it also assumed the ongoing business of the publishing company. Apple Computer has made several six-figure buys of finished product that do not include any rights to source code.

In making the announcement, Mitch Kapor, president of Micro Finance Systems and author of the two software packages, indicated that most of the proceeds from the sale would be pumped back into Micro Finance to fuel research and development of new software products.